The generalized conjugacy problem for virtually free groups

Pedro V. Silva

University of Porto
(Centre of Mathematics, Faculty of Sciences)

York, 28th January 2009

Joint work with **Manuel Ladra González** (*University of Santiago de Compostela*).

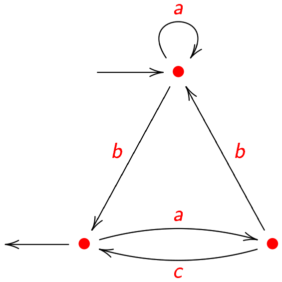
The free group

- A - finite alphabet
- π - congruence on $(A \cup A^{-1})^*$ generated by

$$\{(aa^{-1}, 1) \mid a \in A \cup A^{-1}\}$$

- $F_A = (A \cup A^{-1})^*/\pi$
- R_A - reduced words on $A \cup A^{-1}$
- $\overline{w}$ - reduced word corresponding to w

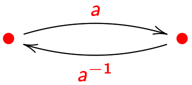
Automata

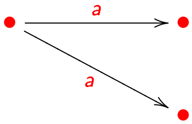


$\mathcal{A} = (Q, i, T, E)$ is an A-automaton if

$$i \in Q,\ T \subseteq Q,\ E \subseteq Q \times A \times Q$$

Inverse automata

- Alphabet $A \cup A^{-1}$
- Duality: 

- Determinism: 

is forbidden ($a \in A \cup A^{-1}$)
- Conectedness

Rational languages

Theorem (Kleene 1956)

$L \subseteq A^*$ is rational if and only if $L = L(\mathcal{A})$ for some finite A-automaton $\mathcal{A}$

- Rat$A$ - set of all rational A-languages
- Underlying idea: *finitely generated sets*

Rational subsets of a group G

- Let $\varphi : (A \cup A^{-1})^* \to G$ be a surjective morphism such that $\varphi(a^{-1}) = (\varphi(a))^{-1}$ for every $a \in A \cup A^{-1}$
- $K \subseteq G$ is rational if $K = \varphi(L)$ for some $L \in \mathrm{Rat}(A \cup A^{-1})$

Theorem (Benois 1969)

If $L \in \mathrm{Rat}(A \cup A^{-1})$, then $\overline{L} \in \mathrm{Rat}(A \cup A^{-1})$

Corollary (Benois 1969)

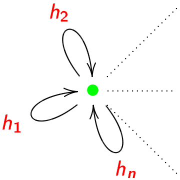
$L \subseteq R_A$ is rational in $(A \cup A^{-1})^*$ if and only if it is rational in F_A

Theorem (Anissimov and Seifert 1975)

$H \leq G$ is rational if and only if it is finitely generated

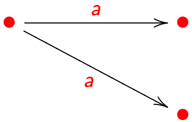
Stallings' construction

$H = \langle h_1, \ldots, h_n \rangle \leq F_A \ (h_i \in R_A)$



Flower automaton

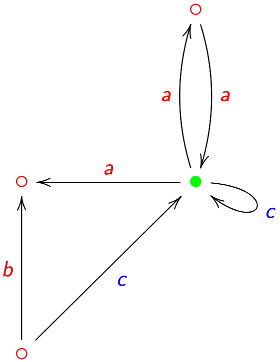
Sucessive folding of edges



until reaching an

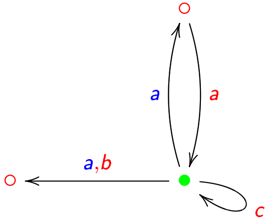
inverse automaton $\mathcal{A}(H)$

Example: $H = \langle a^2, ab^{-1}c, c \rangle$



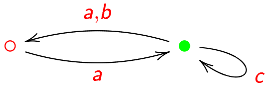
Flower automaton

Example: $H = \langle a^2, ab^{-1}c, c \rangle$



Folding 1

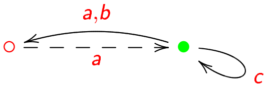
Example: $H = \langle a^2, ab^{-1}c, c\rangle$



Folding 2

Properties

- Confluence: the folding order is irrelevant
- Generalized word problem: given $u \in R_A$, we have $u \in H$ if and only if $u \in L(\mathcal{A})$
- Computation of bases through a maximal subtree:



Base: $\{a^2, ba, c\}$

- ...

Variants of the conjugacy problem

- $\mathrm{Aut}\,G$ - automorphism group of G
- Conjugacy problem: given $g, h \in G$, decide if $g = xhx^{-1}$ for some $x \in G$
- Twisted conjugacy: given $g, h \in G$ and $\varphi \in \mathrm{Aut}\,G$, decide if $g = xh\varphi(x^{-1})$ for some $x \in G$.
  - Free group: solution by Bogopolski, Martino, Maslakova and Ventura (2006)
- Generalized conjugacy: given $g \in G$ and $K \in \mathrm{Rat}\,G$, decide if $xgx^{-1} \in K$ for some $x \in G$.
- Generalized twisted conjugacy: given $g \in G$, $K \in \mathrm{Rat}\,G$ and $\varphi \in \mathrm{Aut}\,G$, decide if $xg\varphi(x^{-1}) \in K$ for some $x \in G$.

The main result

$\varphi \in \mathrm{Aut}G$ is

- inner if there exists $z \in G$ such that $\varphi(g) = zgz^{-1}$ for every $g \in G$
- virtually inner if φ^n is inner for some $n \geq 1$

Theorem 1

Let $g \in F_A$, $K \in \mathrm{Rat}F_A$ and $\varphi \in \mathrm{Aut}F_A$ virtually inner. Then $\mathrm{Sol}(g, \varphi, K) = \{x \in F_A \mid xg\varphi(x^{-1}) \in K\}$ is rational and effectively constructible.

Since it is decidable whether or not $L \in \mathrm{Rat}F_A$ is empty, we can decide if there exists some solution.

Virtually free groups

- G is virtually free if G has a finite index subgroup F which is free
- We may assume that $F \trianglelefteq G$ and $G = Fb_0 \cup \ldots \cup Fb_m$
- For $i = 1, \ldots, m$, we define $\varphi_i \in \mathrm{Aut} F$ by $\varphi_i(u) = b_i u b_i^{-1}$. Since $|G/F| = m+1$, we have $b_i^{m+1} \in F$ and so φ_i is virtually inner.
- The automorphisms φ_i determine to a large extent the structure of G

Structure of rational subsets

Proposition (Silva 2002)

Let $G = Fb_0 \cup \ldots \cup Fb_m$ be a f.g. virtually free group with $F_A = F \trianglelefteq G$. Then $\mathrm{Rat}\, G$ consists of all the subsets of the form

$$\bigcup_{i=0}^{m} L_i b_i \qquad (L_i \in \mathrm{Rat} F_A).$$

Moreover, the components L_i may be effectively computed from a rational expression of L and a standard presentation of G.

Conjugacy in virtually free groups

From Theorem 1, and using the preceding decomposition, we obtain:

Theorem 2

Let G be a virtually free group, $g \in G$ and $K \in \mathrm{Rat}\, G$. Then $\mathrm{Sol}(g, K) = \{x \in G \mid xgx^{-1} \in K\}$ is rational and effectively constructible.

Generalization of Moldavanskii's Theorem

Theorem 3

Let G be a virtually free group and $H_1, \ldots, H_n, K_1, \ldots, K_n \leq_{f.g.} G$. Then $S = \{x \in G \mid \forall i = 1, \ldots, n \quad xH_ix^{-1} = K_i\}$ is rational and effectively constructible.

It follows from Theorems 1, 2 and 3 that we can decide the existence of solutions belonging to any subset C for which it is decidable whether it intersects an arbitrary rational subset

In particular, we can decide the existence of solutions with context-free restrictions

Simplification

Theorem 1 is a consequence of

Theorem 1A

Let $K \in \mathrm{Rat} F_A$ and $\varphi \in \mathrm{Aut} F_A$ be virtually inner. Then $\{x \in F_A \mid x^{-1}\varphi(x) \in K\}$ is rational and effectively constructible.

The following well-known result turns out to be very useful:

Bounded Reduction Lemma

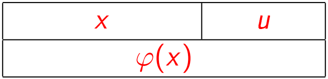
Let $\varphi \in \mathrm{Aut} F_A$. Then there exists $M_\varphi > 0$ such that, whenever $uv \in R_A$, the reduction of $\varphi(u)\varphi(v)$ involves at most M_φ letters of $\varphi(u)$ (and of $\varphi(v)$).

The key

The key to the proof of Theorem 1A lies within

Theorem 1B

Let $\varphi \in \mathrm{Aut} F_A$ be virtually inner. Then $U_\varphi = \{u \in R_A \mid \varphi(x) = xu \text{ for some } x \in R_A\}$ is finite.



If there were no reduction...

If there were no reduction between x^{-1} and $\varphi(x)$, it would be easy to compute the solutions of $x^{-1}\varphi(x) \in K$:

- Let $\mathcal{A} = (Q, q_0, T, E)$ be an automaton with language $\overline{K}$
- For each $q \in Q$, we want to determine all the $x \in R_A$ such that there exist paths

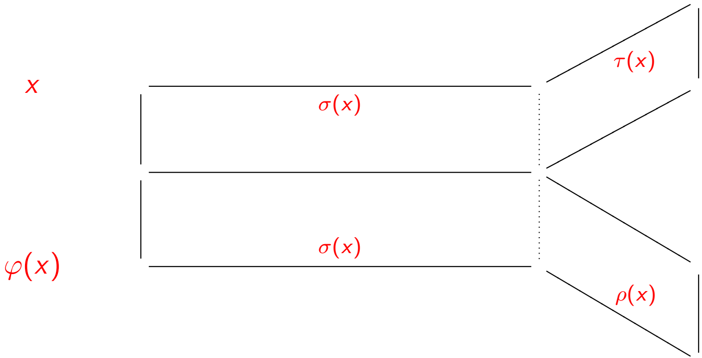
$$q_0 \xrightarrow{x^{-1}} q \xrightarrow{\varphi(x)} t \in T$$

  in $\mathcal{A}$
- The solution is given by

$$x \in \bigcup_{q \in Q} (L(Q, q_0, q, E))^{-1} \cap \varphi^{-1}(L(Q, q, T, E)) \cap R_A,$$

  which is rational by the closure properties of $\mathrm{Rat}(A \cup A^{-1})$

But reduction does exist!

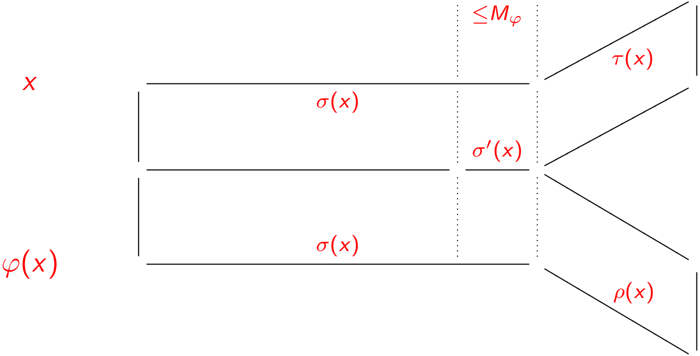


- $\overline{x^{-1}\varphi(x)} = (\tau(x))^{-1}\rho(x)$
- However, if $\tau(x) \neq 1$ and $|\rho(x)| > M_\varphi$, there is no further reduction when we extend x: the situation becomes analogous to the non-reduction case

The role of U_φ and its dual

- The crucial step takes place when $\tau(x) = 1$ or $|\rho(x)| \leq M_\varphi$
- The fact of U_φ and its dual V_φ being finite (a certain $V'_\varphi \supset V_\varphi$, in fact) allows us to consider only finitely many configurations $(\tau(x), \rho(x))$ before reaching the post-reduction situation.
- By the Bounded Reduction Lemma, the evolution of the configuration $(\tau(x), \rho(x))$ when we extend x depends only of a suffix $\sigma'(x)$ of $\sigma(x)$ of length $\leq M_\varphi$.

The configuration $(\sigma'(x), \tau(x), \rho(x))$



The last obstacle

- The algorithm combines thus classification by the configurations $(\sigma'(x), \tau(x), \rho(x))$ with post-reduction analysis, both components involving finite automata
- But there remains a problem: the proof of Theorem 1B is non-constructive, following from topological compactness arguments
- Therefore the algorithm must be conceived in order to overcome that difficulty. The price to pay is the high technical complexity of this part of the proof.
- We give now a brief sketch of the proof of Theorem 1B ($U_\varphi = \{u \in R_A \mid \varphi(x) = xu \text{ for some } x \in R_A\}$ is finite)

The prefix metric

- Given $u = u_1 \dots u_n, v = v_1 \dots v_m \in F_A$ reduced, let

$$r(u,v) = \begin{cases} \min\{i \in \mathbb{N} \mid u_i \neq v_i\} & \text{if } u \neq v \\ \infty & \text{if } u = v \end{cases}$$

and $d(u,v) = 2^{-r(u,v)}$

- d is an ultrametric on F_A
- Let $(\widehat{F_A}, \widehat{d})$ be the completion of (F_A, d)
- $\partial F_A = \widehat{F_A} \setminus F_A$ is said to be the boundary of F_A.

Properties of $\widehat{F_A}$

- $\widehat{F_A}$ is compact
- ∂F_A may be viewed as the set of infinite reduced words on $A \cup A^{-1}$
- $\widehat{d}$ may be defined analogously to d
- every $\varphi \in \mathrm{Aut} F_A$ admits a unique continuous extension $\widehat{\varphi}$ to $\widehat{F_A}$: the union of φ with a permutation of ∂F_A

The fixed point subgroup

Given $\varphi \in \mathrm{Aut} F_A$, let

$$\mathrm{Fix}\varphi = \{g \in F_A \mid \varphi(g) = g\} \leq F_A.$$

- $\mathrm{Fix}\varphi$ is finitely generated (Cooper 1987, Gersten 1984)
- $\mathrm{Fix}\varphi$ is effectively constructible (Maslakova 2003)

Dynamics of the fixed points of $\widehat{\varphi}$

$\alpha \in \text{Fix}\widehat{\varphi}$ is

- singular if it is a limit point of $\text{Fix}\varphi$
- an attractor if

$$\exists \varepsilon > 0 \; \forall \beta \in \widehat{F_A} \; (d(\alpha,\beta) < \varepsilon \;\Rightarrow\; \lim_{n\to\infty} \widehat{\varphi}^n(\beta) = \alpha)$$

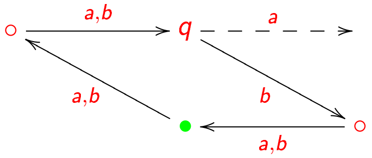
Theorem (Gaboriau, Jaeger, Levitt and Lustig 1998)

Every $\alpha \in \text{Fix}\widehat{\varphi}$ is among the following types:

- singular
- attractor for $\widehat{\varphi}$
- attractor for $\widehat{\varphi^{-1}}$

Decomposition of the solution space

- Let $H = \mathrm{Fix}\varphi$ and $\mathcal{A}(H) = (Q, \bullet, \bullet, E)$
- For each $q \in Q$, we fix a geodesic $\bullet \xrightarrow{g_q} q$ in $\mathcal{A}(H)$
- Let
$$J = \{(q,a) \in Q \times (A \cup A^{-1}) \mid qa = \emptyset\}$$



- Then
$$R_A = (\dot{\bigcup}_{q\in Q}\overline{Hg_q})\ \dot{\bigcup}\ (\dot{\bigcup}_{(q,a)\in J}\overline{Hg_q}aR_A \cap R_A)$$

Compactness

- We can now fix $(q, a) \in J$ and restrict to the domain

$$Y = \{v \in R_A \mid g_q a \leq v \leq \varphi(v)\}.$$

- Since $\widehat{F_A}$ is compact, every infinite subset of Y has a limit point α
- We can prove that α must be a non-singular fixed point which is eventually periodic (as an infinite word)
- Further topological arguments lead to the existence of a bound on $|\varphi(v)| - |v|$

Open problems

Problem 1

Is it decidable, given $g \in F_A$, $K \in \mathrm{Rat} F_A$ and $\varphi \in \mathrm{Aut} F_A$, whether or not $\mathrm{Sol}(g, \varphi, K) \neq \emptyset$?

Problem 2

Is the generalized conjugacy problem decidable for cyclic extensions of f.g. free groups?